



## GTS Computer Service

PO Box 222  
Haskell, NJ 07420  
Phone 973 835-4738  
E-mail [service@gtscomputerservice.com](mailto:service@gtscomputerservice.com)  
Web <http://www.gtscomputerservice.com>

---

## How to Use your Malware Tools

Revised June 14, 2014

See also the companion document “Understanding, Preventing, and Removing Malware”

### General Information

Due to the widespread problem of computer malware (malicious software) infections, GTS routinely installs the excellent free utility programs discussed below for your ongoing protection and maintenance. These programs, which are run manually, are for use in addition to your antivirus program and will not conflict with it.

**WARNING:** When downloading and installing the free versions of these programs, decline free trials of the ‘Pro versions’ and automated updating offers to keep them fully free.

---

### **SpywareBlaster**

Purpose: Provides additional protection against common malware. Good supplement to your antivirus program.

Source: <http://www.brightfort.com/spywareblaster.html>

### How to Use

Periodically download updated protections and enable them as follows:

- Launch the program and click “Download Latest Protection Updates” (near the bottom of the program window).
- On the updates screen click the ‘Check for Updates’ button.
- If a new Update is available it will be downloaded. (If not, there will be a message that there are no new updates available and you can close the program.)
- Under the Update Successful message click “Enable Protection for all Unprotected Items”
- When the enable process finishes, exit the program.

### How Often to Use:

Recommend running once or twice per month (frequency of released updates varies).

---

### **Malwarebytes Anti-Malware**

Purpose: Malware detection and removal.

Source [http://www.malwarebytes.org/products/malwarebytes\\_free](http://www.malwarebytes.org/products/malwarebytes_free) (Look for the Download Free Version button)

**Note:** This program is especially fast and effective. For this reason I recommend running it first if you suspect infection and for periodic maintenance.

### How to Use

**Note:** The recently released version 2 of Malwarebytes changed the user interface. Use the appropriate instructions below for your version. If you are using Version 1, I recommend updating to the new version 2. You can use the link above to download and install it.

#### Version 2.x

- On the Dashboard tab (The program will open by default to this page.) Click Update Now on the Database Version line.
- Once updated, click the Scan Now button in the lower right to run the scan. The “Threat Scan,” the default type, will run fastest and is generally sufficient. If you wish to change it, use the Scan icon on the top bar.
- When the scan is finished click the “Quarantine All” button (on lower left) if any items were found.

- .You may be advised that a reboot is required to finish malware removal and, if so, should permit it.

#### VERSION 1.x

- Launch the program and download updates by clicking on the Updates tab and “Check for Updates” button.
- After updating, click on the Scanner tab and select the Scan type - the Quick scan will run fastest and is generally sufficient. Then click the Scan button, and the program will guide you through the remaining steps..
- You may be advised that a reboot is required to finish malware removal and, if so, should permit it.

#### How Often to Use:

Approximately monthly and anytime you think there may be an infection.

---

#### **SuperAntiSpyware Free Edition** (a manual / help file is available at the web site shown below.)

Purpose: Malware detection and removal.

Source: <http://www.superantispyware.com/>

#### How to Use:

- Launch the program and download updates by clicking on the “Check for Updates” button.
- Click the “Scan your computer button.” Select the Scan type - the Quick scan will run fastest and is generally adequate. The complete scan is more thorough and takes much longer to run.
- When the scan is finished any items found will be listed on a summary screen. Click OK. Then Click next and follow prompts to remove them. Note there will be a check box next to each item found to mark it for removal or keeping. It is generally recommended that all items be removed. If you are advised that SuperAntiSpyware requires a reboot to finish cleaning, allow it to do so.

#### How Often to Use:

Approximately monthly and anytime you think there may be an infection.

---

#### NOTES

1. These programs have other options not discussed here. This document summarizes the most important functions. For more information consult the program’s help file or web site.
2. It can be difficult for users to evaluate items in the list of Malware found by scanners. It is possible, though rare, for an item deletion to cause a problem. It’s best to delete all items found.. The programs provide a quarantine feature to reverse changes if problems should result.
3. Malware infections have become continually more pervasive and difficult to remove. These tools are very valuable for protection and ongoing maintenance, but if your PC is massively infected, professional help will often be required.
4. If there are multiple user accounts on your computer, it is best to run Malware scans and protections under each user.
5. This document may be updated from time to time and will be available on the GTS Computer Service website.
6. Newer versions of these programs are periodically released and are available though their web sites. (The download links occasionally change. You can always find the latest on the links page of <http://www.gtscomputerservice.com>.) It is important to use the latest versions for the most effective protection.